

Blockchain Security Monthly Recap of June: \$95.18M lost in attacks



Beosin · [Follow](#)

4 min read · Jul 10



It's time for our monthly security report! According to Beosin EagleEye, in June 2023, the number of various security incidents and the amount involved increased significantly compared with May 2023. In this month, more than 24 typical security incidents occurred and the total loss of various security incidents was about \$95.18 million, which is up about 480% compared with last month. The Rug Pull loss was about \$4.87 million, which is down about 89% compared with last month.

The largest security incident in June came from the Atomic Wallet wallet theft, with a loss of at least \$67 million. The second largest security incident was the alleged attack by the crypto prime brokerage firm Floating Point Group, which lost \$20 million in cryptocurrency. Neither of the above two major security incidents disclosed the reason for the theft. In June, the number of rug pull incidents decreased significantly, but there

were still 3 incidents in which the amount of escape exceeded \$1M. Users need to be more careful.

DeFi

『13』 Typical Security Incidents

№1 On June 1, Cellframe Network was under price manipulation attack and the attacker made a profit of 245 BNB (about \$74,000).

№2 On June 1, DD Coin was attacked with a loss of \$126,000.

№3 On June 7, MURATIAI was attacked and lost about \$70k.

№4 On June 11, Sell Token on BNB Chain suffered a flash loan attack with a loss of \$94,000.

№5 On June 11, Floating Point Group was under network attack and lost about \$20M.

№6 On June 11, Atlantis Loans was under governance attack with a loss of \$2.5M.

№7 On June 12, Sturdy Finance was attacked with a loss of \$700,000.

№8 On June 15, Hashflow was hacked by a whitehat with a loss of \$600,000. Users can withdraw their stolen funds.

№9 On June 17, PawnFi, a lending protocol, was hacked with a loss of \$800,000.

№10 On June 18, Midas Capital was attacked and the attacker made a profit of \$600,000.

№11 On June 19, ARA was hacked with a loss of \$125,000.

№12 On June 24, ShidoGlobal was attacked with a loss of \$230,000.

№13 On June 28, Themis, a lending protocol, was attacked by oracle manipulation and the attacker made a profit of \$370,000.

Exchange

『1』 Typical Security Incidents

№1 On June 30, BiSwap's contract had a vulnerability causing a loss of \$865000.

Wallet Security

『2』 Typical Security Incidents

№1 On June 3, multiple Atomic Wallet users said that their assets were stolen and the total loss was about \$67M. The reason is still unknown.

№2 Mystic Stealer, a cryptocurrency theft software targeting browsers, browser extensions, and well-known wallets such as MetaMask, Coinbase Wallet, Binance, Rabby Wallet, OKX Wallet, and OneKey, was used to hack users.

Rug Pull/Crypto Scam

『4』 Typical Security Incidents

№1 On June 7, the contract of USEA token had a backdoor and the contract deployer made a profit of \$1100,000 after a Rug Pull.

№2 On June 19, VPANDA DAO had Rug Pull twice and lost about \$1.13M.

№3 On June 20, Zera had a Rug Pull and the fraud made a profit of \$280,000.

№4 Chibi Finance, built on Arbitrum, had a Rug Pull and lost about \$1M. The funds have been transferred into Tornado Cash.

Crypto Crime

『3』 Typical Security Incidents

№1 On June 23, ZachXBT tweeted that the \$6.3m NFT rug pull Animoon was currently under criminal investigation by the French authorities.

№2 On June 24, CFTC charged William Koo Ichioka for defrauding investors of \$21M in crypto ponzi scheme.

№3 South Korean police arrested three and charged another 64 with alleged fraud related to what they say is “a typical Ponzi scheme” that lured victims to invest up to \$127M in a company that claimed to distinguish pet dogs by their noses.

Others

『1』 Typical Security Incidents

№1 Beosin found a critical vulnerability in Move VM, which can cause total network shutdown and potential hard fork in Sui, Aptos, and other public blockchains. Now the vulnerability has been fixed.

In view of the current new situation in the field of blockchain security, Beosin concludes:

Generally, in June 2023, the number of various security incidents and the amount involved increased significantly compared with May. The total loss of various security incidents was about 95.18 million dollars, which is up about 480% compared with May.

User security issue deserves special attention in this month. The Atomic Wallet wallet security incident caused a huge amount of money loss. Mystic Stealer, a cryptocurrency theft software targeting well-known wallets such as MetaMask, Coinbase Wallet, Binance, Rabby Wallet, OKX Wallet, and OneKey, was used to hack users. It is recommended that users choose official channels when downloading programs, keep the mnemonic/private key well, and always pay attention to the reminders of security companies. About 90 percent of attacks in June were due to contract vulnerabilities. It is recommended that project teams complete professional smart contract audits before launching their projects.

Meanwhile, Beosin has issued the Global security report of the first half year of 2023 and welcome to read and share your opinions.

Beosin is a leading global blockchain security company co-founded by several professors from world-renowned universities and there are 40+ PhDs in the team. It has offices in Singapore, South Korea, Japan and other 10+ countries. With the mission of “Securing Blockchain Ecosystem”, Beosin provides “All-in-one” blockchain security solution covering Smart Contract Audit, Risk Monitoring & Alert, KYT/AML, and Crypto Tracing. Beosin has already provided security for 2000+ blockchain companies, audited more than 3000 smart contracts and protected our customers’ assets worth of \$500 billion.

Contact

If you need any blockchain security services, welcome to contact us:

[Official Website](#) [Beosin EagleEye](#) [Twitter](#) [Telegram](#) [Login](#) | [InCareer](#)